UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/647,644	08/25/2003	Mark Eric Obrecht	6002-00602	2528

86942 7590 07/31/2009

Meyertons, Hood, Kivlin, Kowert, Goetzel/Symantec
P.O. Box 398
Austin, TX 78767-0398

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
07/31/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patent_docketing@intprop.com
ptomhkkg@gmail.com

Office Action Summary	Application No.	Applicant(s)	
	10/647,644	OBRECHT ET AL.	
	Examiner	Art Unit	
	SYED ZIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 May 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *105,107,109-115,117,118,127-156,159,162-166 and 168-185* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *105,107,109-115,117,118,127-156,159,162-166 and 168-185* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is responsive to Applicant's amendment and remarks received on 5/13/2009. Claims 168-185 have been added. Claims 105,107, 109-115, 117-118 and 127-156, 159, 162-166, and 168-185 are pending.

Response to Arguments

Applicant's arguments filed on May 13, 2009 have been fully considered but they are not persuasive because of the following reasons:

1. Regarding Claims 105,107, 109-115, 117-118 and 127-156, 159, 162-166, and 168-185 applicant argued that the system Kouznetsov and Chess does not teach "first plurality of detection routines", and "selecting an active program, executes each of the recited first and second plurality of detections routines, and, upon completion, categorizes the code under investigation using results of the executed detection routines"

This is not found persuasive. The cited system clearly teaches and describes a dynamic computer virus detection system that monitors runtime state within defined computing environment, and tracks sequence of execution of monitored execution for each application. A histogram describing the occurrence

of specific execution event sequence characteristic of computer virus behavior for each application, is also created (Kouzentsov: col. 5, line 18 to col. 6, line 30, and Chess: col. 5, line 55 to col. 6, line 35).

Therefore, the examiner asserts that cited prior art(s) does teach or suggest a method and apparatus for detecting malicious code in an information handling system as recited in independent and dependent claims. Accordingly, rejections for claims 20-35 are respectfully maintained.

.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 105, 107, 115, 117-118, and 127-167 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kouznetsov, (U.S. Patent No. 6,973,577), in view of Chess et al., (U.S. Patent No. 6,772,346 and Chess hereinafter).

Regarding claims 105, 115, 117, 127-128, 151-152, and 159-167, Kouznetsov discloses a computer-implemented method comprising:

selecting an active program on a computer system as code under investigation (i.e., wherein code under investigation is each of the incoming system calls 91,92, and 93 generated by the applications 33, 34, and 35 (shown in figure 2))), wherein

the program is running on an operating system of the computer system (col. 5, lines 18-65 and col. 6, lines 1-30); and

executing each of the first and second plurality of detection routines on the operating system of the computer system(i.e., static analyzer 52 and dynamic analyzer 53)(col. 4, lines 47-58), wherein said executing includes:

applying the detection routine to the code under investigation to obtain a result, weighting such result to obtain a score indicative of whether the code under investigation has characteristics and/or behaviors typically associated with malicious code (i.e., static analyzer 52 performs behavior checking and generates alerts and histograms only if patterns of suspicious events are observed. Dynamic analyzer 53 analyzes histograms and identifies behavioral repetitions within the histograms which indicate behavior characteristic of a computer virus/compromise)(col. 4, lines 38-67 and col. 5, lines 1-7);

using the score (i.e., the results indicated by static analyzer 52 and dynamic analyzer 53) to categorize the code under investigation with respect to the likelihood of the code under investigation compromising the security of the computer system (i.e., computer viruses are self-replicating program code which

often carry malicious and sometimes destructive payloads and "malware" can include Trojan horses, hoaxes, and spam mail - col. 1, lines 45-48)(col. 5, lines 18-67 and col. 6, lines 1-30);

using the score to categorize the code under investigation with respect to the likelihood of the code under investigation compromising the security of the computer system (i.e., computer viruses are self-replicating program code which often carry malicious and sometimes destructive payloads and "malware" can be categorized in the following: Trojan horses, hoaxes, and spam mail - col. 1, lines 45-48)(col. 5, lines 18-67 and col. 6, lines 1-30).

Kouznetsov does not explicitly disclose a weighing functionality that scores/determines the monitored events/code under investigation as valid/non-malicious code.

However, Chess discloses applying a detection routine to the code under investigation to obtain a result, weighting such result to obtain a first score indicative of whether the code under investigation has characteristics and/or behaviors typically associated with malicious code with valid code (i.e., files determined to be non-malicious)(col. 5, lines 55-67 and col. 6, lines 1-21), and applying a second detection routine to the code under investigation to obtain a second result, weighting such second result to obtain a second score indicative of whether the code under investigation has characteristics and/or behaviors typically associated with malicious code (col. 6, lines 19-29);

Chess further discloses upon completing the executing of the first and second plurality of detection routines, using the first **and/or** second scores to

categorize the code under investigation with respect to the likelihood of the code under investigation compromising the security of the computer system (i.e., the filtering step may include the steps of determining whether a file contains known malicious code that is correctly handled by an existing protection definition)(col. 5, lines 55-67 and col. 6, lines 1-35).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Kouznetsov with teachings of Chess because it would allow scoring/determining the monitored events/code under investigation as valid/non-malicious and invalid/malicious code as disclosed by Chess. One of ordinary skill in the art would have been motivated by the suggestion of Chess to filter out undesirable mails (i.e., files) from client inboxes (Chess, col. 9, lines 23-30).

Regarding claims 107 and 118, Kouznetsov discloses the method of claim 105, further comprising:

After categorizing the selected active program, selecting an active program on a computer system as code under investigation (i.e., wherein code under investigation is each of the incoming system calls 91,92, and 93 generated by the applications 33, 34, and 35 (shown in figure 2))), wherein the program is running on the computer system (col. 5, lines 18-65 and col. 6, lines 1-30); and

and successively executing each of the first and second plurality of detection routines on the operating system of the computer system(i.e., static analyzer 52 and dynamic analyzer 53)(col. 4, lines 47-58).

Regarding claim 129, Kouzentsov discloses the method of claim 105, further comprising:

determining from the score (i.e., repetitions of suspicious behavioral patterns) that the code under investigation is malicious code (col. 5, lines 43-58 and col. 6, lines 63-67 and col. 7, lines 1-10).

Chess discloses determining from the scores (i.e., matches between code under investigation and the records of database 210 of known non-malicious files or the records of database 220 of known malicious code descriptions) that the code under investigation is malicious code (col. 6, lines 5-35).

Regarding claim 130, Kouzentsov discloses the method of claim 129, wherein the malicious code does not have a known signature (i.e., a knowledge of specific, pre-identified computer viruses would not be necessary because behavioral patterns typical of computer viruses are observed. An example of malicious code with unknown signature is polymorphic viruses) (col. 2, lines 1-2 and lines 21-29).

Regarding claim 131, Kouzentsov discloses the method of claim 105, wherein the detection routine examines the behavior of the suspicious code

under investigation (i.e., static analyzer 52 performs behavior checking and generates alerts and histograms, wherein "behavior checking" is monitoring the occurrence of an event from the events list and dynamic analyzer 53 analyzes histograms and identifies behavioral repetitions within the histograms which indicate behavior characteristic of a computer virus, wherein such histograms are not know virus signatures associated with any virus)(col. 4, lines 47-67 and col. 5, lines 1-6).

Regarding claim 132, Chess discloses the method of claim 131, wherein the detection routine examines the behavior of the valid and suspicious code under investigation (col. 5, lines 55-67 and col. 6, lines 1-29).

Regarding claim 133, Kouzentsov discloses the method of claim 105, wherein the detection routine is not specific to the code under investigation (col. 4, lines 15-37).

Regarding claims 135, 142 and 147, Chess discloses the method of claim 105, wherein the determination is made from the first and second scores that the code under investigation is valid code (i.e., files determined to be non-malicious)(col. 5, lines 55-67 and col. 6, lines 1-21).

Regarding claim 138, Kouzentsov discloses the method of claim 105, wherein determination is made from the score that the code under investigation

is suspicious code, wherein suspicious code has not been determined to be either valid or malicious code (i.e., the categories of the events that are monitored, e.g., events 1-9, col. 5, lines 25-40 may or may not be malicious depending on the repetitions of suspicious behavioral patterns ... the observed group of suspicious events could “potentially” be malicious)(col. 4, lines 38-67 and col. 5, lines 1-67 and col. 6, lines 1-30).

Regarding claim 139, Kouzentsov discloses the system of claim 127, further comprising program instructions executable by the processor to:

determining from the score (i.e., repetitions of suspicious behavioral patterns) that the code under investigation is malicious code (col. 5, lines 43-58 and col. 6, lines 63-67 and col. 7, lines 1-10).

Regarding claims 140, 160, and 161, Kouznetsov discloses the system of claim 139, wherein the malicious code is a previously unknown malicious code (i.e., a knowledge of specific, pre-identified computer viruses would not be necessary because behavioral patterns typical of computer viruses are observed. An example of malicious code with unknown signature is polymorphic viruses) (col. 2, lines 1-2 and lines 21-29).

Regarding claim 142, Chess discloses the system of claim 127, further comprising program instructions executable by the processor to:

determine from the first and second scores that the code under investigation is valid code (i.e., files determined to be non-malicious) (col. 5, lines 55-67 and col. 6, lines 1-21).

Regarding claims 144 and 149, Kouzentsov discloses the system of claim 127, further comprising program instructions executable by the processor to:

determining from the score that the code under investigation is suspicious code (i.e., the categories of the events that are monitored, e.g., events 1-9, col. 5, lines 25-40 may or may not be malicious depending on the repetitions of suspicious behavioral patterns ... the observed group of suspicious events could "potentially" be malicious) (col. 4, lines 38-67 and col. 5, lines 1-67 and col. 6, lines 1-30).

Regarding claim 145, Kouzentsov discloses the memory medium of claim 128, further comprising program instructions executable to:

determining from the score (i.e., repetitions of suspicious behavioral patterns) that the code under investigation is malicious code (col. 5, lines 43-58 and col. 6, lines 63-67 and col. 7, lines 1-10).

Chess discloses determining from the scores (i.e., matches between code under investigation and the records of database 210 of known non-malicious files or the records of database 220 of known malicious code descriptions) that the code under investigation is malicious code (col. 6, lines 5-35).

Regarding claim 146, Kouzentsov discloses the memory medium of claim 145, wherein the malicious code is a previously unknown type of malicious code (i.e., a knowledge of specific, pre-identified computer viruses would not be necessary because behavioral patterns typical of computer viruses are observed. An example of malicious code with unknown signature is polymorphic viruses)(col. 2, lines 1-2 and lines 21-29).

Regarding claim 147, Kouzentsov discloses the memory medium of claim 128, further comprising program instructions executable to:

Determine from the first and second scores that the code under investigation is valid code (i.e., static analyzer 52 performs behavior checking and generates alerts and histograms only if patterns of suspicious events are observed)(col. 4, lines 38-67 and col. 5, lines 1-40).

Regarding claims 134, 136, 137, 141, 143, 148, 150, 153-158, and 162-166, Kouzentsov discloses determining from the score (i.e., repetitions of suspicious behavioral patterns) that the code under investigation is malicious code (col. 5, lines 43-58 and col. 6, lines 63-67 and col. 7, lines 1-10).

Chess further discloses wherein the determination that the code under investigation is malicious code is based on the first score not exceeding a valid code threshold value (i.e., matches between code under investigation and the records of database 210 of known non-malicious files) and the second score exceeding a malicious code threshold value (i.e., matches between code under

investigation and the records of database 220 of known malicious code descriptions) (col. 6, lines 5-35). Chess further discloses clustering files within each classification by using a code-similarity metric to determine the similarity of the possibly-malicious code in each file to the corresponding code in the other files and grouping together those files which are closest according to the metric (col. 7, lines 33-46).

Regarding claim 149, Kouzentsov discloses the memory medium of claim 128, further comprising program instructions executable to:

determine from the first and second scores that the code under investigation is suspicious code (col. 4, lines 38-67 and col. 5, lines 1-40).

Regarding claim 168-185, Kouzentsov discloses wherein:

each of the detection routines within the first and second plurality of detection routines gathers a different type of information about the code under investigation, and wherein the first and second pluralities of detection routines are not themselves running on the operating system of the computer system in a manner that prevents the code under investigation from infecting the computer system (col. 4, line 38 to col. 6, line30).

there is at least one detection routine within the collective first and second pluralities of detection routines that, when executed, obtains information about the code under investigation by accessing the operating system of the computer system via an API of the operating system (col. 4, line 38 to col. 6, line30).

the first and second pluralities of detection routines collectively include a first detection routine that determines a behavior of the code under investigation and a second detection routine that determines a characteristic of the code under investigation (Kouzentsov: col. 5, line 18 to col. 6, line30, and Chess: col. 5, line 55 to col. 6, line 35).

further comprising: for each of a plurality of additional programs running on an operating system of the computer system:

execute each of the first and second pluralities of detection routines on the operating system of the computer system relative to that additional program; use results of the execution of the first and second pluralities of detection routines to categorize that additional program as to the likelihood of that additional program compromising the security of the computer system (col. 5, line 18 to col. 6, line 30).

Claims 109-114 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kouznetsov, (U.S. Patent No. 6,973,577), in view of Chess et al., (U.S. Patent No. 6,772,346 and Chess hereinafter), in further view of Hill et al., (U.S. Patent No. 6,088,804 and Hill hereinafter).

Regarding claims 109-114, Kouznetsov discloses the method of claim 105, wherein the malicious code includes monitoring software (i.e., events such

as system calls having the ability to monitor system input/output activities are monitored)(col. 5, lines 18-67 and col. 6, lines 1-30).

Chess discloses wherein the malicious code can include computer viruses, worms, or Trojan Horses (col. 3, lines 51-53).

Hill further discloses that security event types may include destructive virus, snooping virus, worm, Trojan Horse, FTP requests, and network overload (col. 5, lines 59-61).

It would have also been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Kouznetsov and Chess with teachings of Hill because it would allow to categorize the code under investigation (i.e., simulated attacks – wherein a simulated attack includes at least one of security event types) with respect to the likelihood of the code under investigation compromising the security of the computer system as disclosed by Hill. One of ordinary skill in the art would have been motivated by the suggestion of Hill to provide knowledge of severity and overall nature of attack (Hill, col. 2, lines 45-60).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
July 28, 2009
/Syed Zia/
Primary Examiner, Art Unit 2431